CLAIMS

WHAT IS CLAIMED IS:

1. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a security check unit coupled to receive a linear address generated during execution of a current instruction, wherein the linear address has a corresponding physical address residing within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of the selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

2. The memory management unit as recited in claim 1, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

3. The memory management unit as recited in claim 2, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein

the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

4. The memory management unit as recited in claim 2, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

5. The memory management unit as recited in claim 1, wherein the security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

6. The memory management unit as recited in claim 1, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of a memory page containing the current instruction.

7. The memory management unit as recited in claim 1, wherein the security check logic is configured to obtain the security attribute of the current instruction from the at least one security attribute data structure.

8. The memory management unit as recited in claim 1, wherein the output signal is a fault signal.

9. The memory management unit as recited in claim 1, wherein the security check unit is configured to receive a set of security attributes of the selected memory page in addition to the security attribute of selected memory page, and to produce the output signal dependent upon: (i) the result of the comparison of the numerical value conveyed by the security attribute of the current instruction to the numerical value conveyed by the security attribute of selected memory page, and (ii) the set of security attributes of the selected memory page.

10. The memory management unit as recited in claim 9, wherein the set of security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=l indicates that both read and write accesses are allowed to the selected memory page.

11. A central processing unit, comprising:

an execution unit operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a linear address generated by the execution unit during execution of a current instruction, wherein the linear address has a corresponding physical address that resides within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the MMU is configured to access the selected memory page dependent upon the output signal.

12. A computer system, comprising:

a memory for storing data, wherein the data includes instructions;

a central processing unit (CPU), comprising:

an execution unit operably coupled to the memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores the data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a linear address generated by the execution unit during execution of a current instruction, wherein the linear address has a corresponding physical address residing within a selected memory page, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain a security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the MMU is configured to access the selected memory page dependent upon the output signal.

13. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction, and configured to use the linear address to produce a physical address within a selected memory page, wherein the paging unit is configured to use the linear address to access at least one paged memory data structure located in the memory to obtain security attributes of the selected memory page, and wherein the paging unit is configured to produce a fault signal dependent upon the security attributes of the selected memory page; and

a security check unit coupled to receive the linear address produced during execution of the current instruction, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

14. The memory management unit as recited in claim 13, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

15. The memory management unit as recited in claim 14, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

16. The memory management unit as recited in claim 14, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

17. The memory management unit as recited in claim 13, wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

18. The memory management unit as recited in claim 13, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of a memory page containing the current instruction.

19. The memory management unit as recited in claim 13, wherein the security check unit is coupled to receive a current privilege level (CPL) of a current task including the current instruction, and configured to produce the output signal dependent upon: (i) the result of the comparison of the numerical values conveyed by the security attribute of the current instruction and the security attribute of selected memory page, and (ii) the CPL of the current task including the current instruction.

20. The memory management unit as recited in claim 13, wherein the physical address within the selected memory page includes a base address and an offset, and wherein the paging unit is configured to obtain the base address from the at least one paged memory data structure.

21. The memory management unit as recited in claim 13, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

22. The memory management unit as recited in claim 13, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

23. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address produced during execution of a current instruction residing within a first memory page, wherein the paging unit is configured to use the linear address to produce a physical address accessed by the current instruction, and wherein the physical address includes a base address of a selected memory page and an offset, and wherein the paging unit is configured to access at least one paged memory data structure located in the memory using the linear address to obtain the base address and security attributes of the selected memory page, and wherein the paging unit is configured to receive a security attribute of the instruction, and wherein the paging unit is configured to produce a fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page; and

a security check unit coupled to receive the security attribute of the instruction, the security attributes of the selected memory page, and the linear address produced during execution of the current instruction, and wherein the security check unit is configured to use the linear address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, to compare a numerical value conveyed by a security attribute of the current instruction to a numerical value conveyed by the additional security attribute of selected memory page, and to produce an output signal dependent upon a result of the comparison; and

wherein the memory management unit is configured to access the selected memory page dependent upon the output signal.

24. The memory management unit as recited in claim 23, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

25. The memory management unit as recited in claim 23, wherein the security attribute of the current instruction comprises a current privilege level (CPL) of a task including the current instruction as defined by the x86 processor architecture.

26. The memory management unit as recited in claim 23, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

27. The memory management unit as recited in claim 23, wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.

28. The memory management unit as recited in claim 23, wherein the security attribute of the current instruction comprises a security context identification (SCID) value, and wherein the SCID value is an integer value greater than or equal to 0 and indicates a security context level of the first memory page containing the current instruction.

29. The memory management unit as recited in claim 23, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

30. The memory management unit as recited in claim 29, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table

directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

31. The memory management unit as recited in claim 29, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes security context identification (SCID) field, and wherein the SCID field includes a plurality of bit positions, and wherein the bit positions form a binary representation of an SCID value, and wherein the SCID value is an integer value greater than or equal to 0, and wherein the SCID value indicates a security context level of a corresponding memory page.

32. A method for providing access security for a memory used to store data arranged within a plurality of memory pages, the method comprising:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page;

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page;

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized;

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized;

accessing at least one security attribute data structure located in the memory using the linear address produced during execution of the instruction to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page;

comparing a numerical value conveyed by an additional security attribute of the first memory page to a numerical value conveyed by the additional security attribute of selected memory page; and

accessing the selected memory page dependent upon a result of the comparing of the numerical values conveyed by the security attribute of the first memory page and the additional security attribute of selected memory page.

33. The method as recited in claim 32, wherein the receiving comprises:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page, and wherein the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture.

34. The method as recited in claim 32, wherein the using comprises:

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

35. The method as recited in claim 31, wherein the combining comprises:

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

36. The method as recited in claim 31, wherein the generating comprises:

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized, wherein the fault signal is a general protection fault (GPF) signal as defined by the x86 processor architecture.

37. The method as recited in claim 31, wherein the accessing comprises:

accessing at least one security attribute data structure located in the memory using the linear address produced during execution of the instruction to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table, and wherein the additional security attribute of the first memory page comprises a security context identification (SCID) value of the first memory page, and wherein the SCID value of the first memory page is an integer value greater than or equal to 0 and indicates a security context level of the first memory page, and wherein the additional security attribute of the selected memory page comprises a security context identification (SCID) value of the selected memory page, and wherein the

SCID value of the selected memory page is an integer value greater than or equal to 0 and indicates a security context level of the selected memory page.